VOLUME 3 GENERAL TECHNICAL ADMINISTRATION

CHAPTER 61 AIRCRAFT NETWORK SECURITY PROGRAM

Section 1 Safety Assurance System: Evaluate the Operator's 14 CFR Parts 121, 121/135, 125, and 129 Aircraft Network Security Program

3-4887 REPORTING SYSTEM(S).

A. Program Tracking and Reporting Subsystem (PTRS) Activity Codes.

- 5315 (initial); and
- 5316 (revision).

B. Safety Assurance System (SAS) Automation. This section is related to SAS Elements 4.6.1 (AW), Avionics Special Emphasis Programs.

3-4888 APPLICABILITY.

A. Aircraft Network Security Program (ANSP) Requirement. The requirement for an ANSP is dependent on aircraft design and intended operation. An aircraft requiring an ANSP is one that is certified with a special condition (SC) reflected on the aircraft Type Certificate Data Sheet (TCDS) requiring operator actions to mitigate electronic security risks. These mandatory actions are found in the design approval holder's (DAH) maintenance or operational procedures as required by the special condition. For the purpose of this chapter, these aircraft will be referred to as "connected aircraft."

B. Connected Aircraft. A connected aircraft operated under Title 14 of the Code of Federal Regulations (14 CFR) parts 121, 121/135, 125, and 129 require an ANSP. Operations under 14 CFR parts 91, 125M, and 135 are not required to have an ANSP. However, parts 91, 125M, and 135, as a condition for issuance of an airworthiness certificate, are required to follow the DAH procedures or instructions for continued airworthiness (ICA) developed to meet SCs addressing electronic system security. The DAH procedures must be included in the maintenance and operational programs.

NOTE: Some aircraft may have an SC for electronic security that applies to the DAH design only and does not require operator action. These aircraft do not need an ANSP or maintenance and operational procedures.

3-4889 OBJECTIVE. This section contains information and guidance that the principal avionics inspectors (PAI) use when evaluating an operator's ANSP. Upon official notification that an operator intends to add connected aircraft to their fleet, the PAI must consult the Flight Standards Service (AFS) Aircraft Maintenance Division, Avionics Branch (AFS-360) at (202) 267-1704. This will provide for early coordination to ensure all program requirements are met prior to issuing operations specification (OpSpec) D301. The PAI is responsible for acceptance of the program with the concurrence of AFS-360. Personnel from the Office of Information and Technology Services (AIT) Security and Privacy Risk Management Staff (AIS-020) will support AFS-360 in the evaluation.

NOTE: Because of this unique application of computer technology, AFS-360 will collaborate with AIS-020 to provide technical information technology (IT) security support. AFS-360 will rely on AIS-020 personnel for their expertise in IT cyber security to assist in evaluating the operator's security program. The PAI will make airworthiness evaluations with assistance and recommendations from the assigned AFS-360 aviation safety inspector (ASI).

NOTE: The PAI may require concurrence of ASIs in other specialties to assure all aspects of training are addressed, and to assure that the full operational impact of the connected aircraft configuration is assessed.

3-4890 GENERAL. This section contains a general overview of the requirements for evaluating an ANSP under parts 121, 121/135, 125, and 129. This section contains information and guidance about granting authorization for an operator's ANSP.

NOTE: OpSpec D301 for part 125 certificate holders does not apply to part 125M Letter of Deviation Authority (LODA) operators. It applies to U.S.-registered aircraft operated under part 129, and does not apply to part 129 operators that do not have U.S.-registered aircraft. It applies to all aircraft operated under part 129, § 129.14.

3-4891 ACTION. The ANSP is authorized in OpSpec D301. Log in to the Web-based Operations Safety System (WebOPSS) and follow on-screen prompts to complete the authorization.

3-4892 NEW USE OF TECHNOLOGY. Previously, aircraft designers used aviation (ARINC 429/629) or Military Standard (MIL-STD) data buses to interconnect flight critical avionics systems. Advance connectivity technology was used only to support the passenger information and entertainment systems, which were physically and logically separated from the flight critical avionics systems. New aircraft designs use advanced technology for the main aircraft backbone connecting flight critical avionics as well as passenger information and entertainment systems in a manner that makes the aircraft an airborne interconnected network.

A. External Systems Access. The architecture of this airborne network may allow read and/or write access to and/or from external systems and networks, such as wireless airline operations and maintenance systems, satellite communications, email, the Internet, etc. Onboard wired and wireless devices may also have access to portions of the aircraft's digital data buses that provide flight-critical functions.

NOTE: The design of these connected aircraft makes it difficult to maintain the certificated configuration of the aircraft without following procedures documented in an ANSP. OpSpec D301 is necessary to verify that operators have the skills, tooling, and procedures in place to accomplish the requirements of the DAH's aircraft operator security guidance.

B. Risk. Connected aircraft have the capability to reprogram flight critical avionics components wirelessly and via various data transfer mechanisms. This capability alone, or coupled with passenger connectivity on the aircraft network, may result in cyber security vulnerabilities from intentional or unintentional corruption of data and/or systems critical to the safety and continued airworthiness of the airplane. Credible examples of risks include the potential for:

- Malware to infect an aircraft system,
- An attacker to use onboard wireless to access aircraft system interfaces,
- Denial of service of wireless interfaces,
- Denial of service of safety critical systems,
- Misuse of personal devices that access aircraft systems, and
- Misuse of off-board network connections to access aircraft system interfaces.

3-4893 REGULATORY REQUIREMENTS. The existing regulations did not anticipate this type of system architecture or electronic access to aircraft systems that provide flight-critical functions. Title 14 CFR and current system safety assessment policy and techniques do not address potential cyber security vulnerabilities that unauthorized access to aircraft data buses and servers could cause. In accordance with 14 CFR part 11, § 11.19, as described in 14 CFR part 21, § 21.16, aircraft network systems are certificated through various means, including but not limited to type certificates (TC) and Supplemental Type Certificates (STC) that include SC requirements of the instructions for continued airworthiness (ICA). Title 14 CFR part 43, § 43.13 requires each person performing maintenance, alteration, or preventive maintenance on an aircraft, engine, propeller, or

appliance to use the methods, techniques, and practices prescribed in the current manufacturer's maintenance manual or ICA prepared by its manufacturer; or other methods, techniques, and practices acceptable to the Administrator. PAIs will determine that an operator's ANSP is in compliance with applicable regulations and manufacturer's instructions. The manufacturer's instructions may be in the form of a recommended aircraft security program, airworthiness limitations (AL), or other instructions.

3-4894 REFERENCES, FORMS, AND JOB AIDS.

A. References (current editions):

- Advisory Circular (AC) 119-1, Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP).
- RTCA DO-326A, Airworthiness Security Process Specification and DO-355, Information Security Guidance for Continuing Airworthiness, at http://www.rtca.org.

B. Forms. None.

C. Job Aids. None.

3-4895 OPERATOR ACTION.

A. Develop an ANSP. Operators of connected aircraft must develop and maintain an ANSP that is sufficiently comprehensive in scope and detail to accomplish the following:

1) Ensure that security protection is sufficient to prevent access by unauthorized sources external to the aircraft.

2) Ensure that security threats specific to the certificate holder's operations are identified and assessed, and that risk mitigation strategies are implemented to ensure the continued airworthiness of the aircraft.

3) Prevent inadvertent or malicious changes to the aircraft network, including those possibly caused by maintenance activity.

4) Prevent unauthorized access from sources onboard the aircraft.

NOTE: AIS-020 will be the focal point for verifying the items in subparagraphs 3-4895A1) through A4).

B. Guidelines for Authorization. Operators of connected aircraft during initial certification (including the addition of new types of connected aircraft) should ensure that the initial compliance statement clearly describes the procedures that the operator will use for the ANSP. The operator must develop a section in its General Maintenance Manual (GMM) or other appropriate manual that provides detailed instruction on:

- Roles and responsibilities, including persons with authority and responsibility;
- Training/qualifications;
- Control of maintenance laptop/ground support equipment access and use;
- Control of access to airport wired and wireless service network;
- Controlling access to Loadable Software Airplane Part (LSAP) librarian resources;
- Creating secure parts signing process and controlling access to private keys;
- Control/monitor of physical access to aircraft;
- Control of aircraft conformity to type design, as amended;
- Provisions for parts pooling and parts borrowing;
- Procedures for part exchanges within its own fleet;

- Event recognition and response;
- Event evaluation process with considerations for program improvements; and
- Security environment description.

C. **Verify.** The PAI should encourage the operator to submit the request for authorization for OpSpec D301, along with ANSP documents at least 60 days prior to planned operation of the connected aircraft. Working with AFS-360, the PAI will verify that the operator has established appropriate event recognition, response processes, and security awareness training within their respective program area.

3-4896 **PROCESS.** PAIs, with assistance from AFS-360, will collaborate with certificate holders to determine the mandatory and recommended requirements of the manufacturer's security document.

A. **Verify the Most Recent Version.** Verify that the certificate holder has the most recent version of the manufacturer's security document. Use the following resources to determine the most recent version:

- Airworthiness Limitation Section (ALS) of the Aircraft Maintenance Manual (AMM).
- Aircraft Certification Office (ACO).
- Aircraft Evaluation Group (AEG).

B. **Compare the Requirements and Recommendations.** Compare the requirements and recommendations in the manufacturer's security document to those in the ANSP. Verify that the certificate holder addresses the requirements, and that any recommendations appropriate to the certificate holder operations are included.

NOTE: It is not necessary for the PAI to verify the technical aspects of data security. AIS-020 will accomplish this during headquarters (HQ) review.

C. **Verify the Appropriate Changes.** Verify that appropriate changes are reflected in the certificate holder maintenance program and that the GMM or equivalent manual is revised accordingly. For example, if an ANSP states there is a process to validate the manufacturer's digital signature on software parts received, that process should be described in the "Parts Receiving" section of the GMM. Also, if ANSP sensitive parts are received from a parts pool, the parts pooling procedures should address this.

D. **Review the ANSP.** During initial implementation of OpSpec D301, the regional specialist is not tasked to review the ANSP.

E. **Complete the Package.** The PAI will submit the request directly to AFS-360, with a courtesy copy to the regional specialist. Whenever possible, to allow for the most timely and efficient review, the ANSP package will be submitted electronically via email with return receipt requested. The AFS-360 ASI will submit the ANSP to the assigned AIS-020 security specialist for a concurrent review. The AFS-360 ASI and/or the AIS-020 security specialist may collaborate directly with the PAI, the certificate holder, or the regional specialist to satisfy any issues or concerns. When satisfied, AFS-360 will return the complete package to the PAI with a cover letter recommending authorization of OpSpec D301. AFS-360 will provide a courtesy copy of the cover letter to the regional Flight Standards specialist.

F. **Data Security Manager.** Although not a requirement for every manufacturer's security document, it is critical that the ANSP identify a data security manager. The identity may be by title, organization, and office in the ANSP, provided the certificate holder submits a letter in writing to the certificate-holding district office (CHDO) with the name and contact information for the data security manager. The ANSP should state that the operator shall notify the CHDO within 5 days of subsequent changes to the data security manager. The data security manager is the person with primary responsibility for the ANSP and serves as the focal point for interface with the Federal Aviation Administration (FAA) regarding data security.

3-4897 MERGERS, ACQUISITIONS, AND PROGRAM CHANGES. When two or more ANSPs consolidate because of a merger or acquisition, the consolidation of those programs is of particular importance. The PAI must give priority to the accurate consolidation of those programs. Once the PAI accepts the surviving program, the operator should take action to ensure security records, reports, and logs are maintained, archived, or transferred as appropriate from the existing program into the surviving program. During this transition, the PAI will determine the time period required for maintaining the two systems in parallel operation. The surviving program should have at least the same capability as the existing program. The integration of the existing and surviving programs must maintain the integrity of the security system.

3-4898 CONTRACT MAINTENANCE PROVIDERS. The operator must ensure the contract maintenance provider complies with its ANSP as required by part 121, § 121.363(b) or part 125, § 125.245. The operator will verify compliance with this requirement by use of the audit process required by its Continuing Analysis and Surveillance System (CASS) and Continuous Airworthiness Maintenance Program (CAMP) as required by §§ 121.373 and 121.374, or § 125.247(e). A certificated repair station (CRS) that performs maintenance, preventive maintenance, or alterations for an operator that has an ANSP authorized under OpSpec D301 must follow the operator's program as required by 14 CFR part 145, § 145.205.

3-4899 TASK OUTCOMES.

A. Complete the PTRS. Use PTRS code 5315 for initial ANSP authorization or 5316 for revision thereof. In the "National Use" field, enter "ANSP Init" for initial authorization or "ANSP Rev" for any revisions to OpSpec D301 or any significant security program revisions even if OpSpec D301 is not revised. The PAI must document all reasons to deny the authorization in the comments section of the PTRS record.

B. Future Activities. Routine surveillance can be found in SAS Elements 4.6.1 (AW), Avionics Special Emphasis Program. PAIs will conduct periodic routine surveillance of an operator's ANSP to verify that the operator maintains network security and that the operator has made no significant changes to the program without PAI concurrence. PAIs will verify that the records and security logs continue to contain the required information to show compliance. If the operator makes changes to the ANSP (even when the change is driven by a revision to the manufacturer's security document), or adds additional models of connected aircraft, the PAI will consult AFS-360 to determine if the program requires reevaluation. In accordance with Volume 3, Chapter 18, Section 2 of this order, any changes requiring reissuance of D301 requires AFS-360 approval. As new connected aircraft are delivered to operators, AFS-360 is taking a proactive approach to reach out to the affected PAIs to inform, and assist them in initial implementation of OpSpec D301.

NOTE: AIS-020 may provide additional recommended surveillance tasks in the future.

RESERVED. Paragraphs 3-4900 through 3-4916.